

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR TELEPHONE ASSIGNED
CALL NUMBER (337) 570-0388 THAT IS
STORED AT PREMISES CONTROLLED
BY T-MOBILE, USA

UNDER SEAL

Case No. 1:22-SW-172

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Michael Jeng, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the account associated with telephone number 337-570-0388 (the “SUBJECT PHONE NUMBER”) that is stored at premises owned, maintained, controlled, or operated by **T-MOBILE, USA** (“TELEPHONE SERVICE PROVIDER”), a wireless provider with legal compliance at 4 Sylvan Way, Parsippany, NJ 07054. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require the TELEPHONE SERVICE PROVIDER to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the SUBJECT PHONE NUMBER, including details pertaining to cellular tower sites it has interacted with in the past.

2. I am employed as a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since June 2, 2017. Currently, I am assigned to a squad that investigates organized criminal enterprises and is based at the Washington Field Office – Northern Virginia

Resident Agency in Manassas, Virginia. As a Special Agent, I am authorized to investigate violations of laws of the United States and am authorized to execute warrants issued under the authority of the United States. My duties with the FBI include but are not limited to: the investigation of alleged violations of federal criminal statutes that involve financial institutions; the investigation of complex financial crimes, including extensive document review, analysis, and witness interviews; and the preparation, presentation, and service of criminal complaints, arrest warrants, and search warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from bank personnel. This affidavit is intended to show that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that Mariano Zamora Lopez (“LOPEZ”), the user of the SUBJECT PHONE NUMBER, has committed violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (conspiracy), and 18 U.S.C. § 1029 (access device fraud), among other crimes (the “Target Offenses”). As described in more detail below, there is also probable cause to believe that LOPEZ used the SUBJECT PHONE NUMBER to commit the Target Offenses. Thus, there is probable cause to search the information described in Attachment A and to seize evidence of the Target Offenses as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the proposed warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711; 18 U.S.C. §§ 2703(a) and (b)(1)(A); and

18 U.S.C. §§ 2703 (c)(1)(A). Specifically, the Court is “a district court of the United States ... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On or about November 20, 2020, CAPITAL ONE BANK (CO) detected an unusually large number of back-to-back cash withdrawal attempts conducted by several CO debit cards at CO automatic teller machines (ATMs) in the Leesburg, Virginia area. CO reviewed surveillance footage from these ATMs and observed that the withdrawals appeared to have been made by one unidentified individual even though the cards were in the names of different people. CO noted that the withdrawals were being conducted by the cards’ magnetic strip as opposed to their chip system. CO also reviewed the transaction history of the debit cards and discovered that they had all been used between on or about November 1, 2020 and November 20, 2020, at a VALERO gas station located at 19503 James Monroe Highway in Leesburg, Virginia (located in Loudoun County). Finally, CO contacted one of the holders of these debit cards and confirmed that he or she had not authorized these withdrawals. CO recognized these as indicators of possible criminal activity and notified the Fairfax County Police Department (FCPD) on the same day.

7. On the same day and after receiving this information from CO, the FCPD contacted the Loudoun County Sheriff’s Department (LCSD) and asked them to inspect the gas pumps at the VALERO gas station, specifically the pumps’ debit/credit card readers. Upon arriving, LCSD deputies were not able to access three of the pumps because their locks had been damaged. On or about November 23, 2020, technicians were able to access the pumps and LCSD deputies were able to recover what appeared to be electronic devices from two of the pumps. These devices were seized by the deputies and turned over to Homeland Security Investigations (HSI).

8. From training, experience, and conversations with other law enforcement officers, your affiant knows that these devices were most likely “skimmers,” which are devices that are attached to a debit/credit card point-of-sale terminal such as those found on gas pumps. They are attached by fraudsters to the electronic wiring of the card readers inside the gas pumps so they are not visible to the public. When users (victims) swipe their credit/debit cards at the pump the skimmer copies the data from the victim cards’ magnetic strip as well as the PIN entered into the gas pump’s keypad. The skimmer stores this data until the fraudster can download it remotely via Bluetooth. Once downloaded, the data can be re-encoded onto any card with a magnetic strip, such as a gift card or a hotel key card. The re-encoded card, in combination with the cards’ PIN that was captured by the skimmer, can then be used by the fraudsters at ATMs and other point-of-sale terminals to access funds in the victim’s account without the victim’s authorization.

9. Through its investigation, CO discovered that approximately seventy-two CO debit cards had been compromised by the skimmers recovered by LCSD from the VALERO gas pumps. The re-encoded cards that had been created from these seventy-two compromised cards were then used to attempt to make purchases and withdrawals from various stores and ATMs in Virginia and Texas from on or about November 6, 2020 to May 5, 2021. In total, \$22,270.03 had attempted to be accessed; however, a number of these transactions were declined due to fraud security measures that CO and other retailers had in place, and only \$2,148.13 had been successfully accessed. Given that CO only had access to information on CO accounts, and that it is likely that cards from other banks had been used at the VALERO gas pumps while the skimmers had been installed, your affiant believes that the actual loss amount may be even higher.

10. On or about December 8, 2020, the Federal Bureau of Investigation (FBI) opened an investigation into the VALERO skimming incident and was joined by the FCPD and HSI.

11. Information from CO showed that two re-encoded CO cards, one ending in -6708 and the other in -4250, were used in attempts to make purchases of approximately \$459.69 each at a TARGET store located in Leesburg, Virginia on or about November 20, 2020, at approximately 8:36 a.m. EST and 8:38 a.m. EST, respectively. Both attempts were declined by CO's fraud security measures. Law enforcement consulted TARGET, which provided surveillance footage from the Leesburg TARGET store that showed these transactions were conducted by an individual wearing a white baseball cap and a headset (PERSON 1) at a self-checkout terminal (see Figure 1, where PERSON 1 can be seen in the bottom right, and Figure 2). PERSON 1 appeared to be accompanied by an individual who wore a dark-colored baseball cap with a white emblem (see Figure 1, where PERSON 2 can be seen in the bottom left, and Figure 2).



Figure 1



Figure 2

12. The footage showed that, when conducting these purchases, PERSON 1 would first insert a card into the point-of-sale terminal's chip reader. He would then take the card out and then swipe a different card through the terminal's strip reader. Then he would appear to look at the back of the swiped card before entering in a PIN to the terminal's keypad. PERSON 1 repeated this process eight times before completing his purchase. Information from TARGET confirmed that PERSON 1 unsuccessfully attempted to use seven different debit cards before the eighth one succeeded. Five of the cards were from WELLS FARGO while one was from NAVY FEDERAL CREDIT UNION. The last two cards were the CO cards ending in -6708 and -4250.¹

13. Footage from TARGET showed that PERSON 1 conducted three additional transactions that totaled \$1,521.80 at the Leesburg TARGET's self-checkout terminal. In every transaction, PERSON 1 repeated the process of inserting a card into the chip reader first before swiping a different card. For one of the transactions, PERSON 1 repeated this process twenty-one times and appeared to ask PERSON 2 for additional cards to swipe before finding one that succeeded. TARGET information showed that PERSON 1 used cards from WELLS FARGO, STATE DEPARTMENT FEDERAL CREDIT UNION, BANK OF AMERICA, SUNTRUST, PNC BANK, FIFTH THIRD BANK, SANDY SPRING BANK, BB&T, NAVY FEDERAL

¹ From training, experience, and conversations with other law enforcement officers, your affiant knows that this is a tactic that fraudsters oftentimes use to withdraw funds from re-encoded cards. This is because skimmers can usually only recreate the data from a debit cards' magnetic strip and cannot recreate the security features from its chip. Point-of-sales terminals oftentimes prefer customers to use chip readers due to their higher level of security. When using re-encoded cards, the fraudsters will oftentimes insert a card with a broken chip into the card's chip reader first. The chip reader, being unable to read the broken chip, will then instruct the fraudster to swipe the card's magnetic strip instead. The fraudster would then usually have the PIN numbers written down so they do not need to memorize them.

CREDIT UNION, M&T BANK, and SONABANK.² Receipts provided by TARGET showed that he used these cards to purchase what appeared to be clothes and pre-paid VISA debit cards.³

14. Footage and information from TARGET also showed PERSON 2 conducting a transaction for \$518.00 at an adjacent self-checkout terminal. For this transaction, PERSON 2 purchased three VISA prepaid debit cards. The footage showed that PERSON 2 would insert a card into the chip reader multiple times before swiping the same card through the reader.

15. TARGET footage showed that PERSON 1 and PERSON 2 entered the Leesburg TARGET together at approximately 8:18 a.m. EST that day (see Figure 3). PERSON 2 left at approximately 9:02 a.m. EST (see Figure 4) while PERSON 1 left at approximately 9:05 a.m. EST (see Figure 5). They departed the TARGET in what appeared to be a dark-colored truck (see Figure 6).



Figure 3

² Your affiant believes that this is another indicator that PERSON 1 used re-encoded cards, as their skimming device likely would have captured information from cards from a variety of banks.

³ From training and experience, your affiant knows that this is a method of laundering fraudulently obtained funds. By using the re-encoded cards to purchase pre-paid VISA cards, PERSON 1 converted funds from the victims' accounts into what would appear to be legitimate pre-paid cards.



Figure 4



Figure 5



Figure 6

16. CO provided law enforcement with information about an attempt to use two of the compromised CO card numbers, one ending in -2867 and the other with -2922, at a CO drive-through ATM located in Leesburg, Virginia on or about November 20, 2020, at approximately 9:24 a.m. EST. Surveillance footage showed an individual wearing what appeared to be a headset and a white baseball cap with a Nike logo, similar to that worn by PERSON 1 as seen in Figure 5, in the passenger side of the vehicle while the driver appeared to use the re-encoded CO cards at the ATM (see circled figure in Figure 7). Footage also showed that they appeared to be in a dark-colored truck (see Figure 8), similar to that seen in Figure 6. CO information showed that one of the re-encoded cards was successfully able to be used to withdraw \$2,000.00.

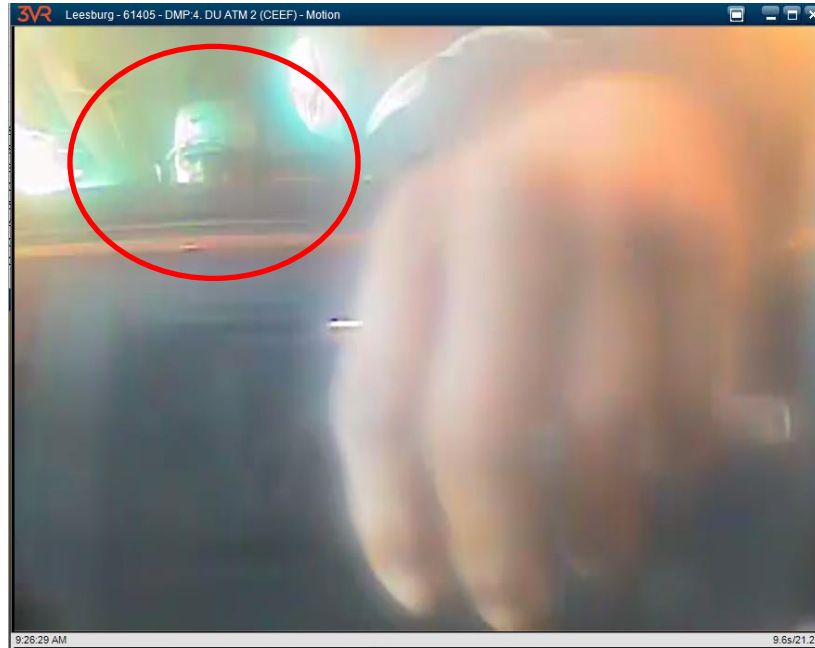


Figure 7



Figure 8

17. CO provided law enforcement with information about an attempt to use two of the compromised CO card numbers, one ending in -1879 and the other with -2922, at a different CO drive-through ATM located in Leesburg, Virginia on or about November 20, 2020, at approximately 2:22 p.m. EST. Surveillance footage showed what appeared to be PERSON 1, again wearing a white baseball cap with a Nike logo and a headset, in the driver's seat using the re-encoded cards at the ATM (see Figure 9). CO information showed that no money was successfully withdrawn during this attempt. CO surveillance footage also showed the license plate of the vehicle driven by PERSON 1 was a Texas plate ending in -3581 (see Figure 10). Law enforcement queried Texas' Department of Motor Vehicles (DMV) and learned that this vehicle was a GMC truck registered to LOPEZ. Law enforcement also obtained LOPEZ's driver's license photograph and height and weight information from the Texas DMV and compared it to TARGET surveillance footage, leading law enforcement to believe that PERSON 2 was LOPEZ.



Figure 9



Figure 10

18. Information from CO showed that, on or about the next day, November 21, 2020, a re-encoded CO card ending in -4963 was used at a CO ATM located in Leesburg, Virginia at or about 11:52 a.m. EST. No funds were able to be withdrawn. CO ATM footage showed that an individual that appeared to resemble LOPEZ conducted this transaction (see Figure 11).

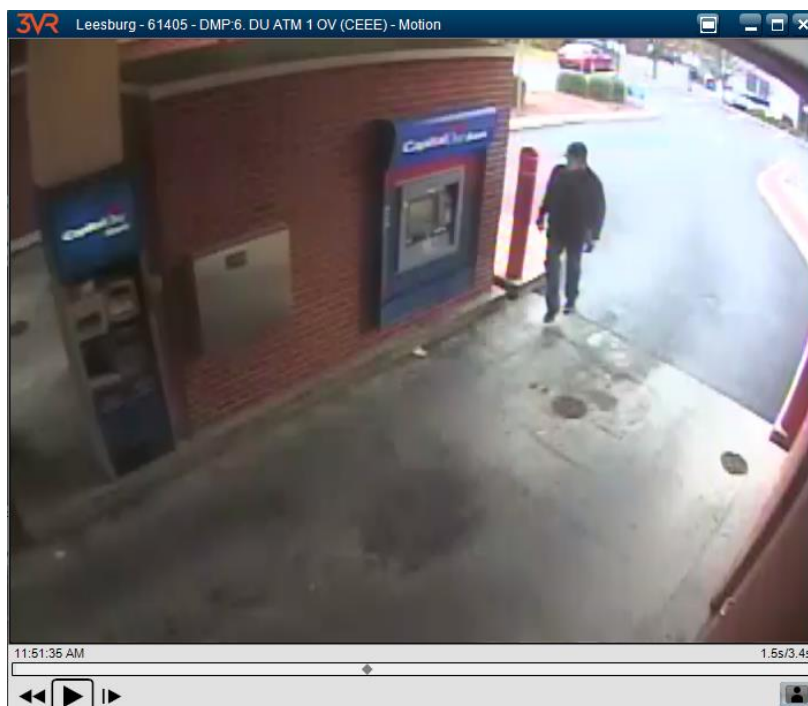


Figure 11

19. Information from CO showed that, on or about November 21, 2020, a re-encoded CO card ending in -1422 was used at a different CO ATM located in Leesburg, Virginia at or about 6:02 p.m. EST in an unsuccessful attempt to withdraw \$2,600.00. CO surveillance footage showed that the user of the card appeared to be wearing the same dark-colored baseball cap with a white emblem (see circled figure in Figure 12) similar to that worn by LOPEZ in Figure 4, and that he appeared to be driving a dark-colored truck (see Figure 13) similar to that seen in Figures 6 and 8–10.

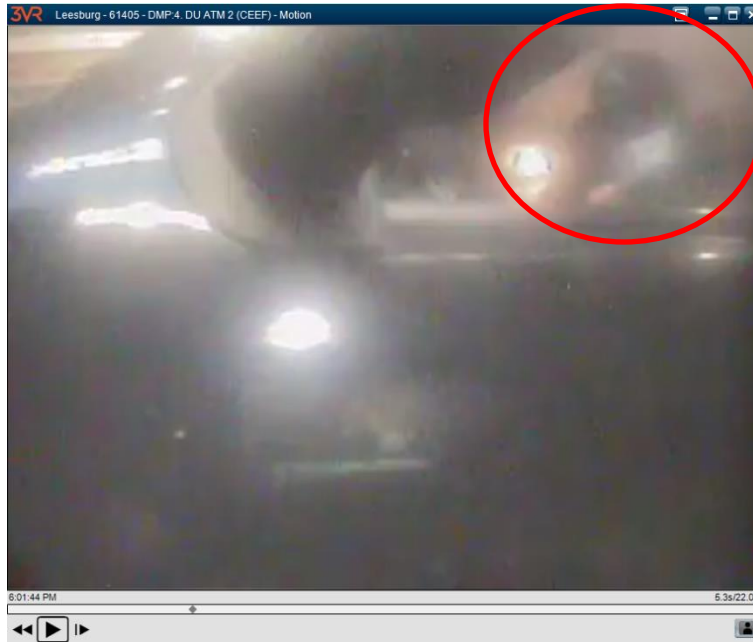


Figure 12

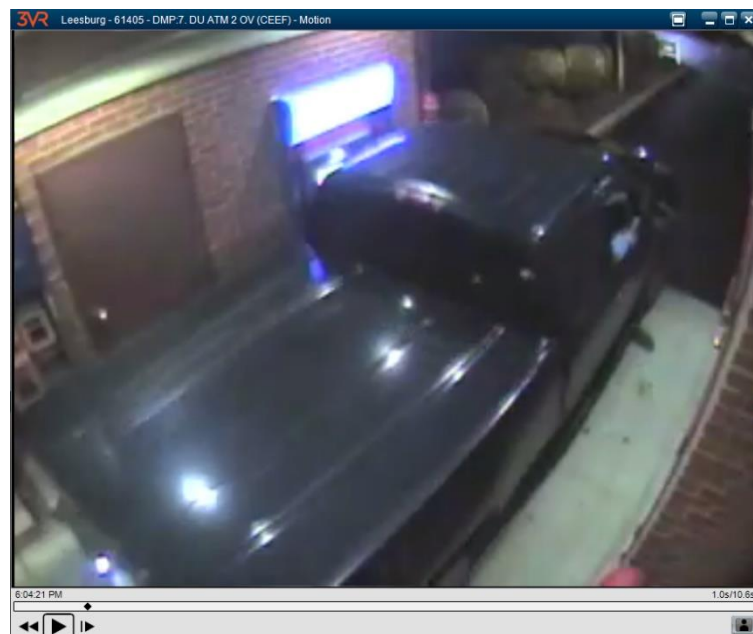


Figure 13

20. Information from CO showed that one re-encoded CO card ending in -0609 was used at a TARGET store located in Leesburg on or about November 21, 2020, at approximately 6:46 p.m. EST, in an unsuccessful attempt to make a purchase of \$466.01. TARGET surveillance showed that this transaction was conducted by LOPEZ, again wearing the dark-colored baseball cap with a white emblem, and PERSON 1, again wearing the white baseball cap with a Nike logo, at a self-checkout terminal (see Figure 14). Footage showed that PERSON 1 again inserted a card into the point-of-sale terminal's chip reader first before swiping a different card through the terminal's magnetic strip reader. PERSON 1 had to repeat this process with thirteen different cards before finding one that would work. These included cards from ESL FEDERAL CREDIT UNION, FIFTH THIRD BANK, DISCOVER, CHASE, WELLS FARGO, CITIBANK, FULTON BANK, USAA, and UNION BANK AND TRUST COMPANY in addition to the CO card. LOPEZ and PERSON 1 also conducted at least two more transactions, one for \$354.39 and the other for \$252.63. CO did not report any of their re-encoded cards were used in these transactions; however, PERSON 1 had to swipe eight different cards to complete these purchases, leading your affiant to believe that they also used re-encoded cards.



Figure 14

21. Information from CO showed that two re-encoded CO cards, one ending in -7702 and the other in -9642, was used at a TARGET store located in Sterling, Virginia on or about November 22, 2020, at approximately 4:27 p.m. EST and 4:37 p.m. EST, to make unsuccessful purchases of \$367.80 and \$463.39, respectively. TARGET surveillance showed that PERSON 1, again wearing a white baseball cap with a Nike logo and headset, was dropped off by a dark-colored GMC truck (see red circled individual in Figure 15 and Figure 16) at this TARGET at approximately 4:14 p.m. EST that day. As with previous TARGET interactions, PERSON 1 repeated the pattern of inserting a card into the chip reader first before swiping with a different card. PERSON 1 again had to swipe multiple cards per transaction before finding one that would work. The surveillance footage from this TARGET store was detailed enough to allow your affiant to observe that PERSON 1 used a card with a distinctive American flag pattern (see Figure 17) to insert into the chip reader each time before swiping, causing your affiant to believe that PERSON

1 deliberately used this card for his scheme because he knew it would cause the terminal to default to the magnetic strip reader.

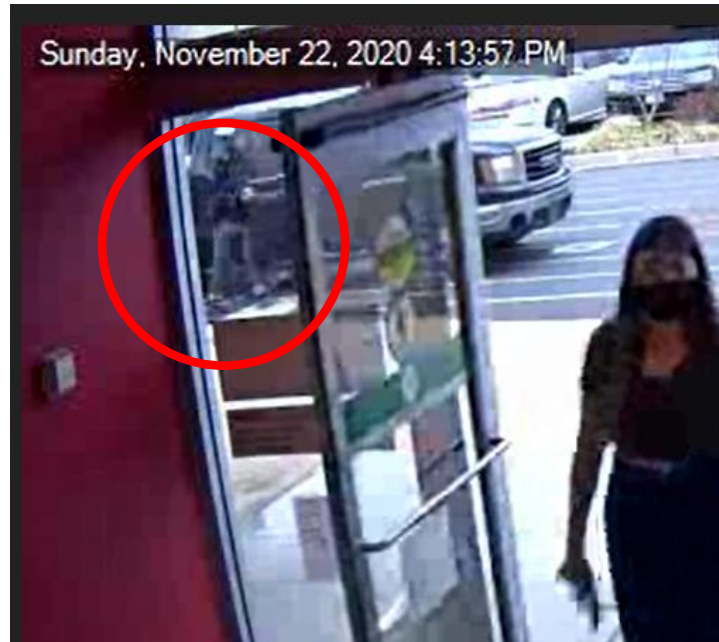


Figure 15



Figure 16



Figure 17

22. CO information showed that, on or about November 23, 2020, at approximately 8:37 p.m. Central Standard Time (CST), one re-encoded CO card ending in -8237 was used at a CO ATM located in Houston, Texas. No funds were withdrawn. CO footage showed an individual wearing glasses (PERSON 3) conducting the transaction (see Figure 18).

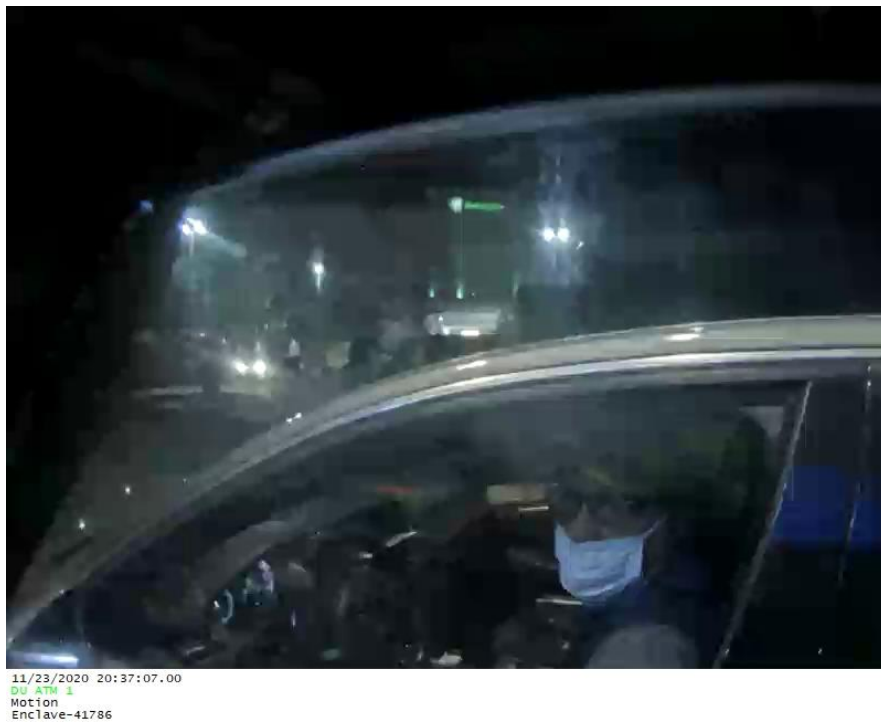


Figure 18

23. CO information showed that, on or about November 28, 2020, three re-encoded CO cards ending in -6599, -8237, and -1525 were used at a different CO ATM in Houston, Texas at or about 12:22 a.m. CST. No funds were successfully withdrawn and CO footage showed what appeared to be PERSON 3, again wearing the same pair of glasses, conducting the transactions (see Figure 19).



Figure 19

24. CO also provided law enforcement with information about an instance in which one re-encoded card ending in -8237 was used at a CO ATM located inside a TARGET store in Houston, Texas on or about November 28, 2020, at approximately 4:35 p.m. CST. Surveillance footage from the ATM showed that it again appeared to be used by PERSON 3 (see Figure 20).

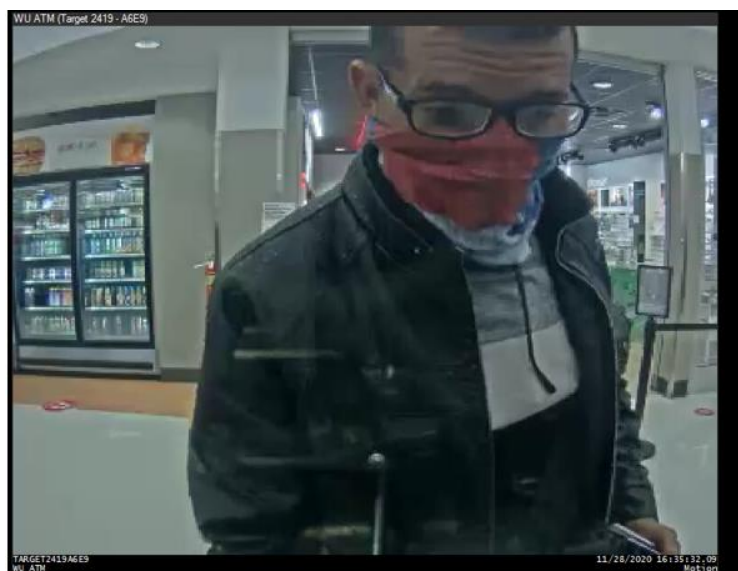


Figure 20

25. Information from CO also showed that, on or about December 4, 2020, at approximately 1:17 a.m. CST, one re-encoded card ending in -4963 was used at a drive-up CO ATM located in Houston, Texas. Surveillance footage showed that the users of the card appeared to be PERSON 1 (again wearing a white baseball cap) and LOPEZ (see Figures 21–23). They attempted to withdraw \$2,260.00 from this card but were unsuccessful.

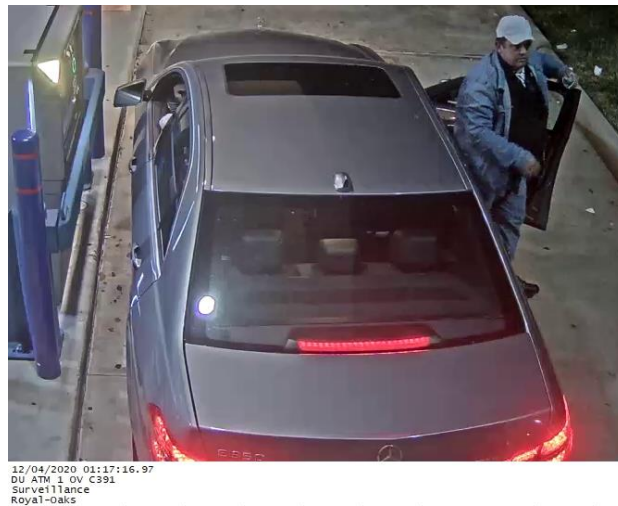


Figure 21



Figure 22



Figure 23

26. CO conducted research on LOPEZ and learned that he was also a CO customer. CO voluntarily provided the telephone number on record for LOPEZ to law enforcement, which ended in -0388. Searches of government and open-source databases showed that this number was associated with LOPEZ. HSI issued an administrative subpoena to the service provider for this number during the events referenced in this affidavit, T-MOBILE, which verified that LOPEZ was the subscriber. T-MOBILE also provided toll records for LOPEZ's number for the period between October 1, 2020 and January 2, 2021, which showed that two other numbers, one ending in -7328 and the other in -1489, were among LOPEZ's most frequently contacted numbers during this period. Law enforcement also learned that these two numbers were serviced by AT&T during the events referenced in this affidavit.

27. A check of government and open-source databases showed that the -1489 number was associated with JUAN MANUEL SOBRINO MONTERO (MONTERO) while the -7328 number was associated with OLIECER PEREZ LEONARD (LEONARD). A criminal history check for MONTERO showed that he was on probation for a prior conviction during the events described in this affidavit. Law enforcement contacted MONTERO's probation officer, who confirmed that MONTERO used the -1489 number. Information from CO also showed that LEONARD was a CO customer and listed the -7328 number as his. Government databases also

returned photographs, age, height, and weight descriptions for MONTERO and LEONARD, which appeared to show that they were identical to PERSONs 1 and 3, respectively.

28. CO provided information to law enforcement regarding an instance in which LEONARD used his personal CO debit card to make a legitimate withdrawal at a CO ATM on or about February 5, 2021. CO provided a still shot from this transaction (see Figure 24) showing that LEONARD bore resemblance to PERSON 3 as seen in Figure 20, to include appearing to wear the same jacket.

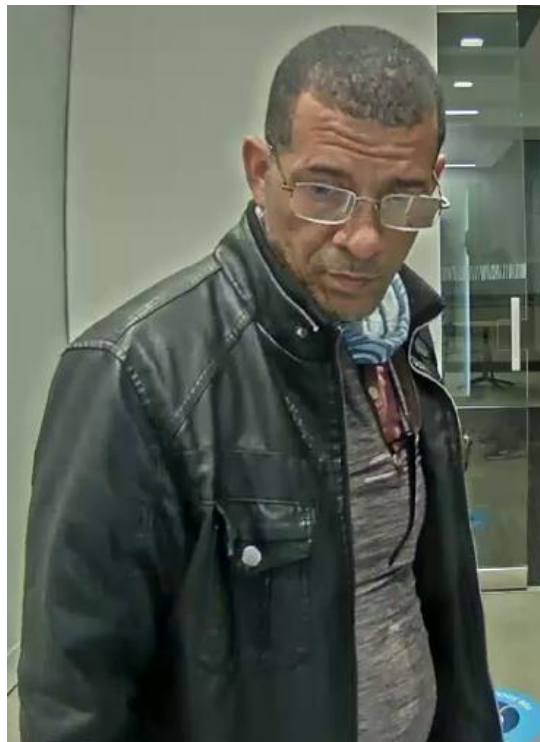


Figure 24

29. Information from CO also reported that, from on or about November 23, 2020 to April 12, 2021, LEONARD deposited fifty-seven money orders into his CO account via a CO ATM located in Houston, Texas. The money orders totaled \$39,661.91. From approximately December 1, 2020 to April 12, 2021, LEONARD accessed these funds via debit card purchases,

ATM withdrawals, and bank transfers. On or about April 20, 2021, CO received notification that these money orders had been purchased with skimmed debit cards, or in other words, re-encoded cards.⁴

30. On or about May 28, 2020, the HOUSTON POLICE DEPARTMENT of Houston, Texas received information from an anonymous tipster regarding MONTERO. According to the tipster, MONTERO was “taking random credit cards in a little computer or software and taking the money...and eventually switches it over to a prepaid card.” The tipster also claimed that MONTERO then used these cards to purchase gas and other items. Your affiant believes that the tipster was describing skimming activity.

31. On or about October 27, 2021, law enforcement executed a search warrant (1:21-SW-739), signed in the Eastern District of Virginia by the Honorable Magistrate Judge Ivan D. Davis, on AT&T for information pertaining to the cellular towers that the numbers -7328 and -1489, believed to be used by LEONARD and MONTERO respectively, interacted with during the events described in this affidavit. AT&T returned results which showed the following:

A. On or about November 20, 2020, at about 8:42 a.m. EST, the -1489 number interacted with a cellular tower located approximately three-quarters of a mile away from the TARGET store referenced in paragraphs 11–15. AT&T information showed that the -1489 number interacted with the same side of the tower that faced the TARGET store. From TARGET surveillance footage, PERSON 1 was known to have been inside this TARGET from approximately 8:18 a.m. EST to 9:05 a.m. EST.

⁴ From training, experience, and conversations with other law enforcement officers, your affiant knows that, because fraud security measures of financial institutions and retailers oftentimes prevent fraudsters from using re-encoded cards at ATMs, fraudsters will oftentimes use the re-encoded cards to purchase money orders from various financial institutions as an alternate means of withdrawing victim funds. Thus, your affiant believes the \$39,661.91 were likely accessed from victim accounts from a variety of banks, including CO.

B. On or about November 20, 2020, at about 2:14 p.m. EST, the -1489 number interacted with a cellular tower located approximately four miles away from the CO ATM referenced in paragraph 17. AT&T information showed that the -1489 number interacted with the same side of the tower that faced the CO ATM. As mentioned in paragraph 17, PERSON 1 was seen on CO ATM footage attempting to use two re-encoded CO cards at this ATM at about 2:22 p.m. EST. At approximately 2:28 p.m. EST, the -1489 number interacted with a different cellular tower, this one a little over a mile away from this CO ATM. Again, the interaction occurred on the same side of the tower that faced the ATM.

C. On or about November 23, 2020, at about 7:14 p.m. CST, the -7328 number interacted with a cellular tower located approximately one and a half miles away from the CO ATM referenced in paragraph 22. As mentioned in paragraph 22, PERSON 3 was seen on CO footage attempting to use one of the re-encoded CO cards at this ATM at approximately 8:37 p.m. CST that day.

D. On or about November 27, 2020, at about 10:42 p.m. CST, the -7328 number interacted with a cellular tower located approximately three and one-quarter miles away from the CO ATM referenced in paragraph 23. AT&T information showed that the -7328 number interacted with the same side of the tower that faced this CO ATM. As mentioned in paragraph 23, CO footage showed that PERSON 3 attempted to use three re-encoded CO cards at this ATM at approximately 12:22 a.m. CST the next day.

E. On or about November 28, 2020, at about 3:39 p.m. CST, the -7328 number interacted with a cellular tower located less than a mile away from the TARGET store referenced in paragraph 24. AT&T information showed that the -7328 number interacted

with the same side of the tower that faced the TARGET store. As mentioned in paragraph 24, PERSON 3 was seen on CO footage inside the TARGET store attempting to use a re-encoded CO card at about 4:35 p.m. CST.

F. On or about December 4, 2020, at about 4:12 a.m. CST, the -1489 number interacted with a cellular tower located less than five miles away from the CO ATM referenced in paragraph 25. As mentioned in paragraph 25, PERSON 1 and LOPEZ were seen on CO footage attempting to use a re-encoded CO card at this ATM at approximately 1:17 a.m. CST earlier this day.

32. By analyzing the results of the AT&T search warrant, as well as comparisons between biographical information obtained for MONTERO and LEONARD with CO and TARGET surveillance footage, your affiant believes that PERSON 1 is MONTERO and PERSON 3 is LEONARD.

33. On or about December 27, 2021, law enforcement executed a search warrant (1:21-SW-845), signed in the Eastern District of Virginia by the Honorable Magistrate Judge John F. Anderson, on T-MOBILE. The search warrant was intended to target the SUBJECT PHONE NUMBER and requested T-MOBILE to provide information pertaining to the cellular towers that the SUBJECT PHONE NUMBER interacted with during the events described in this affidavit so that law enforcement could conduct an analysis on LOPEZ's whereabouts like had been done for MONTERO and LEONARD, as described in paragraph 32. However, upon execution and receiving results from T-MOBILE, law enforcement discovered that they mistakenly requested information for telephone number 337-570-0338, which is one digit off from the SUBJECT PHONE NUMBER. Law enforcement is preparing this affidavit in support of a new search warrant to T-MOBILE to rectify this mistake.

34. Law enforcement also learned that the SUBJECT PHONE NUMBER changed service providers from T-MOBILE to another provider on or about February 4, 2021.

35. In my training and experience, I have learned that the TELEPHONE SERVICE PROVIDER is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for the TELEPHONE SERVICE PROVIDER's subscribers may be located on the computers of the TELEPHONE SERVICE PROVIDER. Further, I am aware that computers located at the TELEPHONE SERVICE PROVIDER contain information and other stored electronic communications belonging to unrelated third parties.

36. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of the TELEPHONE SERVICE PROVIDER for weeks or months.

37. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS") and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by the TELEPHONE SERVICE PROVIDER for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

38. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long-distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers, or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

39. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

40. Providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they

provide service, including cell site data, also known as “tower/face information” or “cell tower/sector records.” Cell site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

41. Based on my training and experience, I know that the TELEPHONE SERVICE PROVIDER can collect cell site data on a historical basis about the SUBJECT PHONE NUMBER. I also know that wireless providers such as the TELEPHONE SERVICE PROVIDER typically collect and retain cell site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

42. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” received a radio signal from the cellular device and thereby transmitted or received the communication in question.

43. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers’ full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers’ Social Security Numbers and dates of birth, all

telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

44. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

45. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were

accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message, to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

46. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require the TELEPHONE SERVICE PROVIDER to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment

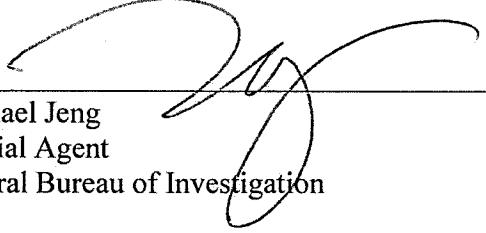
B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on the TELEPHONE SERVICE PROVIDER.

48. Based on the forgoing, I request that the Court issue the proposed search warrant.

Respectfully submitted,



Michael Jeng
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by telephone
in accordance with Fed. R. Crim. P. 4.1
this 16th day of March 2022.

The Honorable Ivan D. Davis
United States Magistrate Judge

Alexandria, Virginia

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with (337) 570-0388 that is stored at premises owned, maintained, controlled, or operated by **T-MOBILE, USA**, a wireless provider with legal compliance at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by T-MOBILE, USA

To the extent that the information described in Attachment A is within the possession, custody, or control of **T-MOBILE, USA**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **T-MOBILE, USA** or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **T-MOBILE, USA** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voicemail, text, and multimedia messages from **November 5, 2020, through February 4, 2021**; stored and presently contained in, or on behalf of the account or identifier, to include the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses).
- b. All existing printouts from original storage of all of the text messages described above.
- c. All transactional information of all activity of the telephone and/or voicemail account described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used that would indicate that the cellular device associated with **(337) 570-0388** was in the vicinity of the events described in this affidavit.

d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message from November 5, 2020, through February 4, 2021.

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account.

f. Detailed billing records, showing all billable calls, including outgoing digits, from November 5, 2020, through February 4, 2021.

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from November 5, 2020, through February 4, 2021.

h. Incoming and outgoing telephone numbers, from November 5, 2020, through February 4, 2021.

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above.

j. All records pertaining to communications between **T-MOBILE, USA** and any person regarding the account or identifier, including contacts with support services and records of actions taken.

k. The date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses).

l. Information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received.

m. Cell site locations and sectors for all outgoing and incoming voice, SMS, MMS, and data transactions.

n. All available timing advance information (e.g., **TruCall** reports), to include cell site, sector, and distance from tower, IP session, and data from **November 19, 2020, through November 26, 2020**.

o. All available mobile data session and IPv6 reports.

The Provider is hereby ordered to disclose the above information to the government within **fourteen days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343, 18 U.S.C. § 1349, and 18 U.S.C. § 1029 involving Mario Zamora Lopez, (337) 570-0388, from **November 5, 2020, through February 4, 2021**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The manufacturing and installation of an access device or skimming device.
- b. The manufacturing and use of stolen debit/credit card information.
- c. The withdrawal of U.S. currency and purchase of gift cards.

d. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation.

e. Evidence indicating the geographic location of the cellular device at times relevant to the investigation.

f. Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation.

g. The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).

h. The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to the installation and removal of a skimming device.